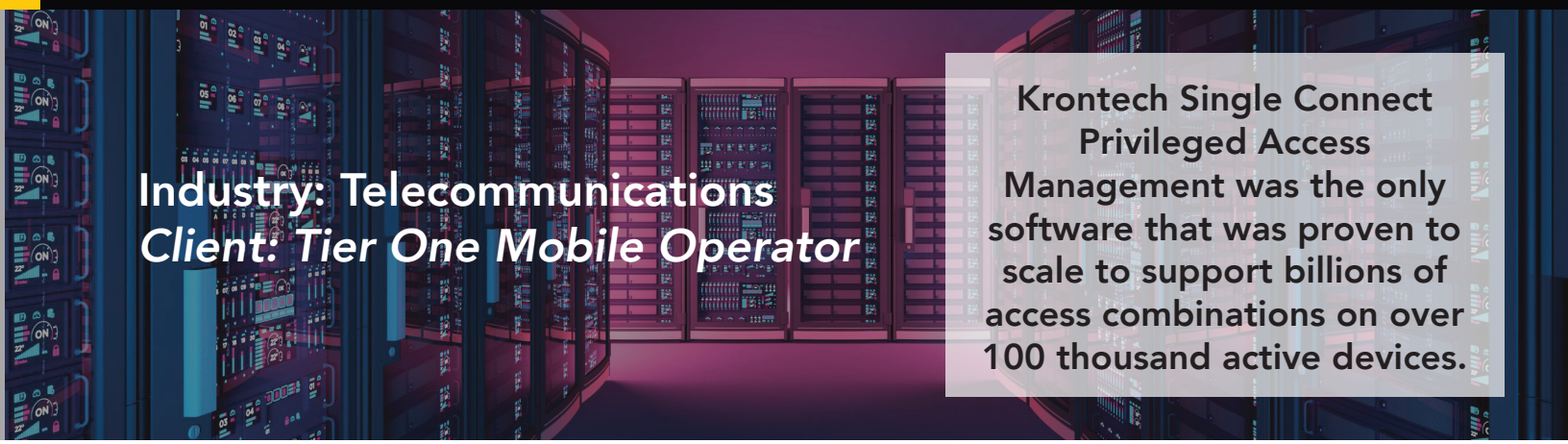

Industry: Telecommunications
Client: Tier One Mobile Operator

Krontech Single Connect Privileged Access Management was the only software that was proven to scale to support billions of access combinations on over 100 thousand active devices.

Introduction

With over 100,000 network devices, 5,000 engineers and operators, and hundreds of vendors requiring access to the infrastructure, controlling privileged access was time consuming, expensive, and risky for this Tier 1 network services provider. Krontech's Single Connect simplified network operations, while securing and controlling access across multiple vendors, with a unified system.

Challenge

Orchestrating 20 different authentication systems (TACACS, RADIUS and LDAP, SQL and others) created massive complexity, particularly as regulations required that the service provider indisputably log every change made to their infrastructure to prevent malicious configurations.

Approach

Simplify and automate access control using Krontech's carrier-grade Single Connect Privileged Access Management tools, implementing a man-in-the-middle solution to secure operations and the network.

Benefits

Simplifed & Secured IT

» Enabled password vault securing over 100,000 active network devices

» Handled and tracked shared accounts

» Enabled over-the-shoulder surveillance on CLI sessions

Saved Money & Met Compliance Standards

» Saved millions of dollars by preventing network downtime

» Generated vital compliance reports for audit

» Ensured that each configuration change on the infrastructure was verified and **approved based on company business policies**

Context, Implementation & Success

Managing internal and external network access is a company's first line of protection concern against network security breaches. Network security teams must control every single action taken on their network infrastructure.

With a mix of IT staff and skill sets, and a broad range of vendors and technology partners needing to access the network operating system, traditional means of controlling access no longer were sufficient. Context aware advance policy definitions for access control needed to be dramatically simplified, automated with improved productivity while securing the system.

» All configuration changes had to be managed in a controlled way and inline with the policies assigned to the operators

» With more than half of the security incidents reported originating from insiders who had privileged access to critical network equipment, tighter internal controls became mission critical

» With no clear and indisputable audit trails of network equipment access, it was a very time-consuming task to find root causes manually and take the required security precautions

Relying on traditional security tools to mitigate the risk of insider and external threats on multi-vendor environments was too risky for this Tier-1 network operator.

To succeed in its highly competitive industry, the operator had to handle these security concerns with a centralized privileged access management solution. Applying a real-world role & responsibility matrix into privileged accounts visually would dramatically improve productivity and outcomes.

With a highly complex, heterogeneous data center environment consisting of more than 50 different vendors and OS technologies, 1,000 UNIX servers, and 1,500 network components, the operator had more than 5,000 privileged accounts and hundreds of thousands of access combinations that needed to be secured and managed. It was vital for them to achieve a better level of privileged access control, enhanced with software and automation, alerts and other productivity tools, reducing manual work and errors.

Privileged access management (PAM) was the key. The operator turned to Krontech because of our years of experience in the domain, our track record implementing and managing many PAM projects for other large operators, and our unique software solutions.

Krontech's solution architecture team designed and delivered a unique set of functions for Privileged Session Management(PSM), which uses Krontech's Single Connect Privileged Access Management technology.

The PSM module is designed to minimize the risk of unauthorized network changes while maintaining audit trails. It reduces risk by guarding and governing the network within an advanced management policy of command, personnel and devices.

The Krontech professional service team gathered all the relevant network access policy information and set up the management platform. In doing so, we covered the complete operational lifecycle of privileged access to network equipment by defining context aware policy sets, generating indisputable session logs and publishing audit reports of operator actions. Single Connect Privileged Session Management module leveraged a "man-in-the-middle" approach to network equipment access and today stands as a bridge between network equipment and users for this operator. As a seamless proxy system, it is managing and monitoring privileged sessions, commands and actions in real-time, and recording them for audit and further purposes.

In the Customer's Own Words

"The Privileged Session Management solution delivered by Krontech reduced workloads and minimized the privileged access security risks, resulting in savings of at least $100,000 a year."

Managing Director,
Network Operations and Security, Large Mobile Service Provider

Learn more about Krontech's Single Connect by visiting krontech.com

About Krontech

Krontech's mission is to support telecom service providers and large enterprises secure their networks with Privileged Access Management software and solutions. We help organizations reduce risks and operate more efficiently.

Krontech is a software company established in 2007, and produces and integrates advanced technology software in the fields of Access Control Systems, Network Packet Brokerage, Streaming Analytics, Fast Data & Real Time Data Processing, and Next-generation Security and Audit. With cost-efficient, flexible, and tailored solutions, Krontech is a respected and proven partner, supporting many Tier-1 telecom service providers and large global enterprises. Krontech is headquartered in New York City with research and development facilities in Istanbul, and regional sales and support offices in Europe, Middle East and Africa, and Asia Pacific.